SSA-547990: Information Disclosure Vulnerabilities in SIPROTEC 4 and SIPROTEC Compact

Publication Date: 2016-05-19
Last Update: 2018-05-15
Current Version: V1.2
CVSS v3.0 Base Score: 5.3

SUMMARY

Information disclosure vulnerabilities in SIPROTEC 4 and SIPROTEC Compact devices could allow an attacker to extract sensitive device information under certain conditions.

Siemens has released firmware updates for EN100 Ethernet module included in SIPROTEC 4 and SIPROTEC Compact devices. Siemens has also released a firmware update for SIPROTEC Compact 7SJ80 with Ethernet Service Interface on Port A. For remaining affected devices, countermeasures are recommended. Siemens will update this advisory when new information becomes available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
EN100 Ethernet module included in SIPROTEC 4: EN100 version V4.26 or lower	Update to V4.27 http://www.siemens.com/downloads/siprotec-4 (click on the plus sign next to the respective model -> “Firmware and Device Drivers” -> “Communication Protocols – IEC 61850” -> “Update EN100 V4.27 for all devices over the EN100 interface” or “Update EN100 V4.27 for all devices over the front interface”)
EN100 Ethernet module included in SIPROTEC Compact: EN100 version V4.26 or lower	Update to V4.27 http://www.siemens.com/downloads/siprotec-compact (click on the plus sign next to the respective model -> “Firmware and Device Drivers” -> “Communication Protocols – IEC 61850” -> “Update EN100 V4.27 over the EN100 interface” or “Update EN100 V4.27 over the front interface”)
SIPROTEC Compact model 7SJ80 with Ethernet Service Interface on Port A: Firmware version V4.75 or lower	Update to V4.76 http://www.siemens.com/downloads/siprotec-compact (click on the plus sign next to 7SJ80 -> “Firmware and Device Drivers” -> “Firmware” -> “Setup_7SJ80x_04.76.01”)
SIPROTEC Compact models 7RW80, 7SJ81, and 7SK81 with Ethernet Service Interface on Port A: All firmware versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

Recommended security guidelines to Secure Substations can be found at:

https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

SIPROTEC 4 and SIPROTEC Compact devices provide a wide range of integrated protection, control, measurement, and automation functions for electrical substations and other fields of application.

The EN100 Ethernet modules are used for enabling process communication and either IEC 61850, PROFINET IO, Modbus TCP, DNP3 TCP or IEC 104 communication with electrical/optical 100 Mbit interfaces for SIPROTEC 4, SIPROTEC Compact and Reyrolle devices.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability CVE-2016-4784

The integrated web server (port 80/tcp) of the affected devices could allow remote attackers to obtain sensitive device information if network access was obtained.

CVSS v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2016-4785

The integrated web server (port 80/tcp) of the affected devices could allow remoteattackers to obtain a limited amount of device memory content if network access was obtained. This vulnerability only affects EN100 Ethernet module included in SIPROTEC4 and SIPROTEC Compact devices.

CVSS v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Aleksandr Bersenev from HackerDom team for coordinated disclosure of CVE-2016-4784
- Pavel Toporkov from Kaspersky Lab for coordinated disclosure of CVE-2016-4785
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for coordination efforts

ADDITIONAL INFORMATION

For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-05-19):	Publication Date
V1.1 (2016-06-30):	Added update information for SIPROTEC Compact 7SJ80; removed SIPROTEC Compact 7SK80 from Affected Products
V1.2 (2018-05-15):	New format; Removed 7SD80 from list of affected products

TERMS OF USE